SALISH BH-ASO POLICIES AND PROCEDURES

Policy Name: PASSWORD PROTECTION **Policy Number:** PS910

Effective Date: 1/1/2020

Revision Dates:

Reviewed Date: 4/5/2023

Executive Board Approval Dates: 7/30/2021

POLICY

The Salish Behavioral Health Administrative Services Organization's (SBH-ASO) privacy and security practices are mandated by state and federal laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

These regulations require that SBH-ASO deploy and maintain a set of policies, practices, and technologies to safeguard confidential information and ensure that such information is not disclosed to anyone without the proper authorization to view or possess such information.

PROCEDURE

Access Codes and Passwords

The confidentiality and integrity of data stored on SBH-ASO computer systems must be protected by access controls to ensure that only authorized workforce members have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. The Kitsap County Information Services Department (Information Services Department) will institute a system of access controls consisting first of a unique identification code and password requirement for each employee with a need to use SBH-ASO computer systems and networks. The characteristics of the password requirement will be established by the Information Services Department.

Information Services Responsibilities

- The Information Services Department shall be responsible for the administration of access controls to all SBH-ASO computer systems.
- The Information Services Department will deploy and maintain a set of system/network access and password procedures that require unique user identification codes and passwords that conform to standardized characteristics.

- The Information Services Department will maintain a list of administrative access codes and passwords and keep this list in a secure area.
- The Information Services Department will assign responsibility for maintenance of the access code and password assignment to a qualified individual in the Information Services Department. Additionally, a back-up staff person of the department will also be assigned these duties as a backup to the primary staff person.

Employee Responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not disclose passwords to others. This should be strictly interpreted by all staff. If a password is requested from an employee, the employee should verify the identity of that person with the Information Services Department staff member responsible for maintenance of the access codes and passwords. If the responsible staff are not available, the employee is instructed not to disclose his/her password.
- Must immediately change passwords if it is suspected that they may have become known to others. In the event that an employee suspects or knows that his/her password has become known to an unauthorized person, the employee should immediately report this event to the following agency staff:
    a. The designated staff person in the Information Services Department responsible for maintenance of access codes and passwords
    b. The Privacy Officer
- Shall not record passwords where they may be easily obtained. Employees shall not display passwords in any area that can be viewed by others. This means practically that passwords should not be written on “sticky” notes on the monitor, placed on paper and taped to the bottom of the keyboard, etc.
- Will change passwords at least every 60 days.
- Should use passwords that will not be easily guessed by others.

Managers’ Responsibility

Managers should notify the Information Services Department in advance whenever an employee leaves the SBH-ASO so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Enforcement

All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to disciplinary action.